Terms used **conglomerated certificate** Found **3,824** of **196,064**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 L3—towards an open learning environment

Torsten Leidig

March 2001 **Journal on Educational Resources in Computing (JERIC)**

Publisher: ACM Press

Full text available: pdf(131.06 KB) Additional Information: full citation, abstract, references, index terms

This article describe the use of dedicated ontology for teaching in the context of the L3 project, a national joint project for deploying further vocational education in Germany. The requirements for the open L3 learning infrastructure are presented in order to motivate our approach to metamodeling learning resources and services by using dedicated ontolgies of pedagogics and didactics. The basic concepts and parts ...

Keywords: adaptive courses delivery, authoring environment for web-based training, didatics, pedagogical ontology, reuse of learning resources

2 Dynamic composition of workflows for customized eGovernment service delivery

Soon Ae Chun, Vijayalakshmi Atluri, Nabil R. Adam

May 2002 **Proceedings of the 2002 annual national conference on Digital government research dg.o '02**

Publisher: Digital Government Research Center

Full text available: pdf(103.86 KB) Additional Information: full citation, abstract, references, citings

Today, many government agencies provide tremendous amount of information and services via the Web, often overwhelming the citizens. Personalization and customization in delivering information and government services remains as a major challenge. In this paper, we present a novel approach for dynamically composing workflows to delivering customized government services to citizens. Such a system is especially important in a government service delivery due to the fact that many autonomous governmen ...

3 Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems

Naftaly H. Minsky, Victoria Ungureanu

July 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 3

Publisher: ACM Press

Full text available: pdf(792.05 KB) Additional Information: full citation, abstract, references, citings, index terms

Software technology is undergoing a transition form monolithic systems, constructed according to a single overall design, into conglomerates of semiautonomous, heterogeneous, and independently designed subsystems, constructed and managed by different organizations, with little, if any, knowledge of each other. Among the problems inherent in such conglomerates, none is more serious than the difficulty to control the activities of the disparate agents operating in it, and the ...

Keywords: coordination of heterogeneous agents, policy enforcement, scalability

4 Privacy policies as decision-making tools: an evaluation of online privacy notices

Carlos Jensen, Colin Potts

April 2004 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '04**

Publisher: ACM Press

Full text available: pdf(292.27 KB) Additional Information: full citation, abstract, references, citings, index terms

Studies have repeatedly shown that users are increasingly concerned about their privacy when they go online. In response to both public interest and regulatory pressures, privacy policies have become almost ubiquitous. An estimated 77% of websites now post a privacy policy. These policies differ greatly from site to site, and often address issues that are different from those that users care about. They are in most cases the users' only source of information.This paper evaluates the usability of ...

Keywords: WWW, consent, e-commerce, privacy, readability, usability

5 Payment systems for hypermedia information systems

S. Bakhtiari, R. Safavi-Naini, R. Gonzalez, H. W. Peter Beadle

October 1996 **ACM SIGSAC Review**, Volume 14 Issue 4

Publisher: ACM Press

Full text available: pdf(416.17 KB) Additional Information: full citation, abstract, references, index terms

Before the transition of the Internet from being primarily an academic and research vehicle to a commercial one can occur, suitable electronic payment systems must be deployed. Currently a variety of different schemes are proposed featuring varying degrees of security. Internet environment requires support for both micro and macro payment systems. It is unlikely that any one scheme can satisfy the requirements of all the intended applications. This paper gives a brief evaluation of the major cat ...

6 Modeling: On the impact of dynamic addressing on malware propagation

Moheeb Abu Rajab, Fabian Monrose, Andreas Terzis

November 2006 **Proceedings of the 4th ACM workshop on Recurring malcode WORM '06**

Publisher: ACM Press

Full text available: pdf(328.87 KB) Additional Information: full citation, abstract, references, index terms

While malware models have become increasingly accurate over the past few years, none of the existing proposals accounts for the use of Network Address Translation (NAT). This oversight is problematic since many network customers use NAT in their local networks. In fact, measurements we collected from a distributed honeynet show that approximately 19% of the infected hosts reside in NATted domains. To account for this fact, we present a model that can be used to understand the impact of varying I ...

Keywords: internet worms, network address translation, network security, private address space

7 Understanding complex information environments: a social analysis of watershed planning

Lisa R. Schiff, Nancy A. Van House, Mark H. Butler

July 1997 **Proceedings of the second ACM international conference on Digital libraries DL '97**

Publisher: ACM Press

Full text available: pdf(1.48 MB) Additional Information: full citation, references, citings, index terms

8 Data access for the masses through OLE DB

José A. Blakeley

June 1996 **ACM SIGMOD Record , Proceedings of the 1996 ACM SIGMOD international conference on Management of data SIGMOD '96**, Volume 25 Issue 2

Publisher: ACM Press

Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents an overview of OLE DB, a set of interfaces being developed at Microsoft whose goal is to enable applications to have uniform access to data stored in DBMS and non-DBMS information containers. Applications will be able to take advantage of the benefits of database technology without having to transfer data from its place of origin to a DBMS. Our approach consists of defining an open, extensible Collection of interfaces that factor and encapsulate orthogonal, reusable portions ...

9 Teaching e-commerce to a multidisciplinary class

Rachna Dhamija, Rachelle Heller, Lance J. Hoffman

September 1999 **Communications of the ACM**, Volume 42 Issue 9

Publisher: ACM Press

Full text available: pdf(211.83 KB) html(26.44 KB) Additional Information: full citation, references, citings, index terms

10 Viewpoint: One more revolution to make: free scientific publishing

Krzysztof R. Apt

May 2001 **Communications of the ACM**, Volume 44 Issue 5

Publisher: ACM Press

Full text available: pdf(72.37 KB) html(21.95 KB) Additional Information: full citation, references, index terms

11 Status report of the graphic standards planning committee

Computer Graphics staff

August 1979 **ACM SIGGRAPH Computer Graphics**, Volume 13 Issue 3

Publisher: ACM Press

Full text available: pdf(15.01 MB) Additional Information: full citation, references, citings

12 Novel uses of Java: Components: a valuable investment for financial engineering, why derivative contracts should be active documents

Markus Reitz, Ulrich Nögel

August 2006 **Proceedings of the 4th international symposium on Principles and practice of programming in Java PPPJ '06**

Publisher: ACM Press

Full text available: pdf(753.76 KB) Additional Information: full citation, abstract, references

Although component-oriented thinking is quite common to software developers, the paradigm's impact beyond its "native" domain is limited. *Financial Engineering*, a fast-growing discipline that combines finance, applied mathematics and computer science, often uses inflexible straightforward implementations for the underlying mathematical descriptions and models. Missing the benefits of modern software technology, even small variations in the financial products portfolio usually induce huge ...

Keywords: Java, Web 2.0, XML, active documents, component-orientation, derivative contracts, financial engineering

13 Web services: Legal research topics within services sciences

Olli Pitkänen

October 2006 **Proceedings of the 2006 conference of the Center for Advanced Studies on Collaborative research CASCON '06**

Publisher: ACM Press

Full text available: pdf(346.12 KB) htm(1.34 KB) Additional Information: full citation, abstract, references

The paper presents a study to define some of the most important legal topics that need to be included in the Services Sciences' research agenda.To analyze what sort of legal challenges the forthcoming services will have, an example of advanced service framework, MobiLife Service Framework, is presented. The framework high-lights especially challenges in privacy and data protection and intellectual property rights.The analysis is complemented with a discussion on some other scenarios and examples ...

14 Genealogical approaches to ethical implications of informational assimilative integrated discovery systems (AIDS) in business

Kamal Dean Pharhizgar, Stephen E. Lunce

November 1994 **Proceedings of the conference on Ethics in the computer age**

Publisher: ACM Press

Full text available: pdf(694.25 KB) Additional Information: full citation, abstract, references, index terms

Development of knowledge-based technological acquisition techniques and customers' information profiles are known as assimilative integrated discovery systems (AIDS) in modern organizations. These systems have access through processing to both deep and broad domains of information in modern societies. Through these systems organizations and individuals can predict future trend probabilities and events concerning their customers. AIDSs are new techniques which produce new information which i ...

15 Barriers to implementing simulation in health care

Julie C. Lowery, Brian Hakes, Lou Keller, William R. Lilegdon, Kal Mabrouk, Frank McGuire

December 1994 **Proceedings of the 26th conference on Winter simulation WSC '94**

Publisher: Society for Computer Simulation International

Full text available: pdf(886.08 KB) Additional Information: full citation, references, citings, index terms

16 Banking

Gerald M. Lowrie

January 1970 **Proceedings of the 1970 25th annual conference on Computers and crisis: how computers are shaping our future ACM '70 , Computers and**

crisis
Publisher: ACM Press
Full text available: pdf(630.62 KB) Additional Information: full citation, abstract

In his opening remarks, Mr. Lowrie said that bankers are considered by some to be staid and conventional, whereas in terms of computer usage the bankers have been far from conventional. From a position in 1960 of perhaps the least significant user of all the Sectors represented at the Conference, banking has become the largest. Excepting the Government Sector, almost 20% of all systems and programming talent works within the Finance Sector.

17 Authentication: An approach to certificate path discovery in mobile Ad Hoc networks
He Huang, Shyhtsun Felix Wu
October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**
Publisher: ACM Press
Full text available: pdf(146.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Public key certificates prove validity and authenticity of their ownership and possibly other properties. Certificate path discovery is the critical process for public key verification in hierarchical public key infrastructure (PKI) diagrams. This process is conventionally done in centralized public key management system such as central CA or directory. However, in an infrastructure-less environment, such as a mobile ad hoc network, no such central service is present due to network dynamics. Tha ...

Keywords: MANET, certificate path discovery, public key infrastructure, security

18 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure
Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

19 XML security: Certificate validation service using XKMS for computational grid
Namje Park, Kiyoung Moon, Sungwon Sohn
October 2003 **Proceedings of the 2003 ACM workshop on XML security XMLSEC '03**
Publisher: ACM Press
Full text available: pdf(7.01 MB) Additional Information: full citation, abstract, references, index terms

A computational grid is a hardware and software infrastructure capable of providing dependable, consistent, pervasive, and inexpensive access to high-end computational resource. There are many ways to access the resources of a computational grid, each with

unique security requirements and implications for both the resource user and the resource provider. Current Grid security Infrastructure using PKI based on SSO. But open grid service Security Infrastructure in Global Grid Forum(GGF) will exten ...

Keywords: GSI, XKMS, XML, XML security, certificate validation, grid, key management, security

20 Using certes to infer client response time at the web server



David Olshefski, Jason Nieh, Dakshi Agrawal
February 2004 **ACM Transactions on Computer Systems (TOCS)**, Volume 22 Issue 1
Publisher: ACM Press

Full text available: pdf(2.30 MB) Additional Information: full citation, abstract, references, citings, index terms

As businesses continue to grow their World Wide Web presence, it is becoming increasingly vital for them to have quantitative measures of the mean client perceived response times of their web services. We present Certes (CliEnt Response Time Estimated by the Server), an online server-based mechanism that allows web servers to estimate mean client perceived response time, as if measured at the client. Certes is based on a model of TCP that quantifies the effect that connection drops have on mean ...

Keywords: Web server, client perceived response time

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

Terms used **conglomerated virtual host certificate** Found **9,701** of **196,064**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Status report of the graphic standards planning committee

Computer Graphics staff

August 1979 **ACM SIGGRAPH Computer Graphics**, Volume 13 Issue 3

Publisher: ACM Press

Full text available: pdf(15.01 MB) Additional Information: full citation, references, citings

2 Security technology and applications: E-business security issues for SMEs in a virtual hosting environment

Neville I Williams

September 2003 **Proceedings of the 1st international symposium on Information and communication technologies ISICT '03**

Publisher: Trinity College Dublin

Full text available: pdf(626.88 KB) Additional Information: full citation, abstract, references

The Small and medium Enterprise (SME) sector is often reliant on external internet services due to their limited internal expertise in technological and other non-core business areas. As a result they are potentially more prone to overlook or be unaware of important security issues when they expand their web presence into the commercial transactions segment of e-business.In this paper the basis of those security issues will be examined with respect to the virtual web hosting environment, to clar ...

Keywords: electronic business, security, small and medium enterprises, virtual web hosting security

3 Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS

Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas

November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**

Publisher: ACM Press

Full text available: pdf(447.59 KB) Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized applications that would otherwise be prone to replay

attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights management (DRM). In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine with a Trusted Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

4 Terra: a virtual machine-based platform for trusted computing

Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh

October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5

Publisher: ACM Press

Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

5 Virtual machines: ReVirt: enabling intrusion analysis through virtual-machine logging and replay

George W. Dunlap, Samuel T. King, Sukru Cinar, Murtaza A. Basrai, Peter M. Chen

December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI

Publisher: ACM Press

Full text available: pdf(1.56 MB) Additional Information: full citation, abstract, references, citings

Current system loggers have two problems: they depend on the integrity of the operating system being logged, and they do not save sufficient information to replay and analyze attacks that include any non-deterministic events. ReVirt removes the dependency on the target operating system by moving it into a virtual machine and logging below the virtual machine. This allows ReVirt to replay the system's execution before, during, and after an intruder compromises the system, even if the intruder rep ...

6 Astrolabe: A robust and scalable technology for distributed system monitoring, management, and data mining

Robbert Van Renesse, Kenneth P. Birman, Werner Vogels

May 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 2

Publisher: ACM Press

Full text available: pdf(341.62 KB) Additional Information: full citation, abstract, references, citings, index terms

Scalable management and self-organizational capabilities are emerging as central requirements for a generation of large-scale, highly dynamic, distributed applications. We have developed an entirely new distributed information management system called Astrolabe. Astrolabe collects large-scale system state, permitting rapid updates and providing on-the-fly attribute aggregation. This latter capability permits an application to locate a resource, and also offers a scalable way to track sys ...

Keywords: Aggregation, epidemic protocols, failure detection, gossip, membership, publish-subscribe, scalability

7 Design and implementation of a distributed virtual machine for networked computers

Emin Gün Sirer, Robert Grimm, Arthur J. Gregory, Brian N. Bershad

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.62 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the motivation, architecture and performance of a distributed virtual machine (DVM) for networked computers. DVMs rely on a distributed service architecture to meet the manageability, security and uniformity requirements of large, heterogeneous clusters of networked computers. In a DVM, system services, such as verification, security enforcement, compilation and optimization, are factored out of clients and located on powerful network servers. This partitioning of system fun ...

8 Distrbuted VEEs: HyperSpector: virtual distributed monitoring environments for secure intrusion detection

Kenichi Kourai, Shigeru Chiba

June 2005 **Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments VEE '05**

Publisher: ACM Press

Full text available: pdf(262.72 KB) Additional Information: full citation, abstract, references, index terms

In this paper, a virtual distributed monitoring environment called *HyperSpector* is described that achieves secure intrusion detection in distributed computer systems. While multiple intrusion detection systems (IDSes) can protect a distributed system from attackers, they can increase the number of insecure points in the protected system. HyperSpector overcomes this problem without any additional hardware by using virtualization to isolate each IDS from the servers it monitors. The IDSes a ...

Keywords: distributed IDS, inter-VM monitoring, virtual machine, virtual network

9 Velnet: virtual environment for learning networking

Bruce Kneale, Ain Y. De Horta, Ilona Box

January 2004 **Proceedings of the sixth conference on Australasian computing education - Volume 30 ACE '04**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(616.15 KB) Additional Information: full citation, abstract, references, citings, index terms

The problems of providing a real, physical specialist laboratory to teach computer networking such as, the lack of funding and physical space and the risks and threats to the network environment and infrastructure, can be solved by the use of a virtual learning environment. Velnet is such a virtual learning environment that we have developed and used successfully. Velnet consists of one or more host machines and operating systems, commercial virtual machine software, virtual machines and their o ...

Keywords: Velnet, computer networking, virtual learning environment

10 A simple virtual organisation model and practical implementation

Lyle J. Winton

January 2005 **Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 ACSW Frontiers '05**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(315.22 KB) Additional Information: full citation, abstract, references, index terms

The development of Grid middleware, such as the Globus Toolkit version 2, reached a level of maturity and stability in which it was possible to create widely distributed resource Grids. Within the last few years various experiences have arisen from the construction of such Grids and so called "testbeds". The purpose of this paper is to highlight some of the problems, propose some simple solutions, and to report on the development of prototype implementations. The focus of this paper is on soluti ...

Keywords: computing, globus, grid, virtual organisations

11 Smart packets: applying active networks to network management

Beverly Schwartz, Alden W. Jackson, W. Timothy Strayer, Wenyi Zhou, R. Dennis Rockwell, Craig Partridge

February 2000 **ACM Transactions on Computer Systems (TOCS)**, Volume 18 Issue 1

Publisher: ACM Press

Full text available: pdf(190.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This article introduces Smart Packets and describes the smart Packets architecture, the packet formats, the language and its design goals, and security considerations. Smart Packets is an Active Networks project focusing on applying active networks technology to network management and monitoring. Messages in active networks are programs that are executed at nodes on the path to one or more target hosts. Smart Packets programs are written in a tightly encoded, safe language specifically des ...

Keywords: active networks

12 VMPlants: Providing and Managing Virtual Machine Execution Environments for Grid Computing

Ivan Krsul, Arijit Ganguly, Jian Zhang, Jose A. B. Fortes, Renato J. Figueiredo

November 2004 **Proceedings of the 2004 ACM/IEEE conference on Supercomputing SC '04**

Publisher: IEEE Computer Society

Full text available: pdf(207.42 KB) Additional Information: full citation, abstract, citings

Virtual machines provide flexible, powerful execution environments for Grid computing, offering isolation and security mechanisms complementary to operating systems, customization and encapsulation of entire application environments, and support for legacy applications. This paper describes a Grid service ¿ VMPlant ¿ that provides for automated configuration and creation of flexible VMs that, once configured to meet application needs, can then subsequently be copied ("cloned") and dynamically in ...

13 Backtracking intrusions

Samuel T. King, Peter M. Chen

February 2005 **ACM Transactions on Computer Systems (TOCS)**, Volume 23 Issue 1

Publisher: ACM Press

Full text available: pdf(647.38 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Analyzing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of steps that occurred in an attack. The goal of BackTracker is to identify automatically potential sequences of steps that occurred in an intrusion. Starting with a single detection point (e.g., a suspicious file), BackTracker identifies files and processes that could have affected that detection point and displays chains of events i ...

Keywords: Computer forensics, information flow, intrusion analysis

14 Agents, interactions, mobility, and systems (AIMS): Using mobile agents as roaming security guards to test and improve security of hosts and networks

Marco Carvalho, Thomas Cowin, Niranjan Suri, Maggie Breedy, Kenneth Ford
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing SAC '04**
Publisher: ACM Press

Full text available: pdf(307.45 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper discusses the design and implementation details of MAST (Mobile Agent-based Security Tool), a new mobile agent-based network security approach. MAST has been designed to support flexible and customizable network security tasks and training. This paper focuses on the implementation details and security aspects of MAST's components, services, and mobile-agent architecture

Keywords: IHMC, MAST, concept maps, knowledge models, mobile agents, network security

15 Secure virtual enclaves: Supporting coalition use of distributed application technologies

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2
Publisher: ACM Press

Full text available: pdf(462.10 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The Secure Virtual Enclaves (SVE) collaboration infrastructure allows multiple organizations to share their distributed application objects, while respecting organizational autonomy over local resources. The infrastructure is transparent to applications, which may be accessed via a web server, or may be based on Java or Microsoft's DCOM. The SVE infrastructure is implemented in middleware, with no modifications to COTS operating systems or network protocols. The system enables dynamic updates to ...

Keywords: Access control, coalition, collaborative system, group communication, middleware, security policy

16 (How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions

Joris Claessens, Bart Preneel, Joos Vandewalle
February 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 1
Publisher: ACM Press

Full text available: pdf(197.96 KB) Additional Information: full citation, abstract, references, citings, index terms

This article investigates if and how mobile agents can execute secure electronic transactions on untrusted hosts. An overview of the security issues of mobile agents is

first given. The problem of untrusted (i.e., potentially malicious) hosts is one of these issues, and appears to be the most difficult to solve. The current approaches to counter this problem are evaluated, and their relevance for secure electronic transactions is discussed. In particular, a state-of-the-art survey of mobile agen ...

Keywords: Mobile agent security, electronic transactions, malicious hosts

17 Backtracking intrusions

Samuel T. King, Peter M. Chen
October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5
Publisher: ACM Press

Full text available: pdf(185.10 KB) Additional Information: full citation, abstract, references, citings, index terms

Analyzing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of steps that occurred in an attack. The goal of BackTracker is to identify automatically potential sequences of steps that occurred in an intrusion. Starting with a single detection point (e.g., a suspicious file), BackTracker identifies files and processes that could have affected that detection point and displays chains of events i ...

Keywords: computer forensics, information flow, intrusion analysis

18 Certificate-based authorization policy in a PKI environment

Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press

Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

19 Automated and certified conformance to responsiveness policies

Joseph C. Vanderwaart, Karl Crary
January 2005 **Proceedings of the 2005 ACM SIGPLAN international workshop on Types in languages design and implementation TLDI '05**
Publisher: ACM Press

Full text available: pdf(615.49 KB) Additional Information: full citation, abstract, references, index terms

Certified code systems protect computers from faulty or malicious code by requiring untrusted software to be accompanied by checkable evidence of its safety. This paper presents a certified code solution to a problem in grid computing, namely, controlling the CPU usage of untrusted programs. Specifically, we propose to endow the runtime system supervising local execution of grid programs with a trusted "yield" operation, and require the untrusted code to execute this operation with at least a ce ...

Keywords: certified code, grid computing, typed assembly language

20 Formalizing the safety of Java, the Java virtual machine, and Java card

Pieter H. Hartel, Luc Moreau
December 2001 **ACM Computing Surveys (CSUR)**, Volume 33 Issue 4
Publisher: ACM Press

Full text available: pdf(442.86 KB) Additional Information: full citation, abstract, references, citings, index terms

We review the existing literature on Java safety, emphasizing formal approaches, and the impact of Java safety on small footprint devices such as smartcards. The conclusion is that although a lot of good work has been done, a more concerted effort is needed to build a coherent set of machine-readable formal models of the whole of Java and its implementation. This is a formidable task but we believe it is essential to build trust in Java safety, and thence to achieve ITSEC level 6 or Common Crite ...

Keywords: Common criteria, programming

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

Terms used **conglomerated internet certificate** Found **3,470** of **196,064**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 L3—towards an open learning environment

Torsten Leidig

March 2001 **Journal on Educational Resources in Computing (JERIC)**

Publisher: ACM Press

Full text available: pdf(131.06 KB) Additional Information: full citation, abstract, references, index terms

This article describe the use of dedicated ontology for teaching in the context of the L3 project, a national joint project for deploying further vocational education in Germany. The requirements for the open L3 learning infrastructure are presented in order to motivate our approach to metamodeling learning resources and services by using dedicated ontolgies of pedagogics and didactics. The basic concepts and parts ...

Keywords: adaptive courses delivery, authoring environment for web-based training, didatics, pedagogical ontology, reuse of learning resources

2 Privacy policies as decision-making tools: an evaluation of online privacy notices

Carlos Jensen, Colin Potts

April 2004 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '04**

Publisher: ACM Press

Full text available: pdf(292.27 KB) Additional Information: full citation, abstract, references, citings, index terms

Studies have repeatedly shown that users are increasingly concerned about their privacy when they go online. In response to both public interest and regulatory pressures, privacy policies have become almost ubiquitous. An estimated 77% of websites now post a privacy policy. These policies differ greatly from site to site, and often address issues that are different from those that users care about. They are in most cases the users' only source of information.This paper evaluates the usability of ...

Keywords: WWW, consent, e-commerce, privacy, readability, usability

3 Modeling: On the impact of dynamic addressing on malware propagation

Moheeb Abu Rajab, Fabian Monrose, Andreas Terzis

November 2006 **Proceedings of the 4th ACM workshop on Recurring malcode WORM '06**

Publisher: ACM Press

Full text available: pdf(328.87 KB) Additional Information: full citation, abstract, references, index terms

While malware models have become increasingly accurate over the past few years, none of the existing proposals accounts for the use of Network Address Translation (NAT). This oversight is problematic since many network customers use NAT in their local networks. In fact, measurements we collected from a distributed honeynet show that approximately 19% of the infected hosts reside in NATted domains. To account for this fact, we present a model that can be used to understand the impact of varying I ...

Keywords: internet worms, network address translation, network security, private address space

4 Payment systems for hypermedia information systems

S. Bakhtiari, R. Safavi-Naini, R. Gonzalez, H. W. Peter Beadle

October 1996 **ACM SIGSAC Review**, Volume 14 Issue 4

Publisher: ACM Press

Full text available: pdf(416.17 KB) Additional Information: full citation, abstract, references, index terms

Before the transition of the Internet from being primarily an academic and research vehicle to a commercial one can occur, suitable electronic payment systems must be deployed. Currently a variety of different schemes are proposed featuring varying degrees of security. Internet environment requires support for both micro and macro payment systems. It is unlikely that any one scheme can satisfy the requirements of all the intended applications. This paper gives a brief evaluation of the major cat ...

5 Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems

Naftaly H. Minsky, Victoria Ungureanu

July 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 3

Publisher: ACM Press

Full text available: pdf(792.05 KB) Additional Information: full citation, abstract, references, citings, index terms

Software technology is undergoing a transition form monolithic systems, constructed according to a single overall design, into conglomerates of semiautonomous, heterogeneous, and independently designed subsystems, constructed and managed by different organizations, with little, if any, knowledge of each other. Among the problems inherent in such conglomerates, none is more serious than the difficulty to control the activities of the disparate agents operating in it, and the ...

Keywords: coordination of heterogeneous agents, policy enforcement, scalability

6 Dynamic composition of workflows for customized eGovernment service delivery

Soon Ae Chun, Vijayalakshmi Atluri, Nabil R. Adam

May 2002 **Proceedings of the 2002 annual national conference on Digital government research dg.o '02**

Publisher: Digital Government Research Center

Full text available: pdf(103.86 KB) Additional Information: full citation, abstract, references, citings

Today, many government agencies provide tremendous amount of information and services via the Web, often overwhelming the citizens. Personalization and customization in delivering information and government services remains as a major challenge. In this paper, we present a novel approach for dynamically composing workflows to delivering customized government services to citizens. Such a system is especially important in a

government service delivery due to the fact that many autonomous governmen ...

7 Teaching e-commerce to a multidisciplinary class

Rachna Dhamija, Rachelle Heller, Lance J. Hoffman
September 1999 **Communications of the ACM**, Volume 42 Issue 9
Publisher: ACM Press
Full text available: pdf(211.83 KB) html(26.44 KB) Additional Information: full citation, references, citings, index terms

8 CERT incident response and the Internet

Katherine Fithen, Barbara Fraser
August 1994 **Communications of the ACM**, Volume 37 Issue 8
Publisher: ACM Press
Full text available: pdf(3.26 MB) Additional Information: full citation, references, index terms

9 Understanding complex information environments: a social analysis of watershed planning

Lisa R. Schiff, Nancy A. Van House, Mark H. Butler
July 1997 **Proceedings of the second ACM international conference on Digital libraries DL '97**
Publisher: ACM Press
Full text available: pdf(1.48 MB) Additional Information: full citation, references, citings, index terms

10 Web services: Legal research topics within services sciences

Olli Pitkänen
October 2006 **Proceedings of the 2006 conference of the Center for Advanced Studies on Collaborative research CASCON '06**
Publisher: ACM Press
Full text available: pdf(346.12 KB) htm(1.34 KB) Additional Information: full citation, abstract, references

The paper presents a study to define some of the most important legal topics that need to be included in the Services Sciences' research agenda.To analyze what sort of legal challenges the forthcoming services will have, an example of advanced service framework, MobiLife Service Framework, is presented. The framework high-lights especially challenges in privacy and data protection and intellectual property rights.The analysis is complemented with a discussion on some other scenarios and examples ...

11 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote
May 2002 **Proceedings of the 2002 annual national conference on Digital government research dg.o '02**
Publisher: Digital Government Research Center
Full text available: pdf(539.99 KB) Additional Information: full citation

12 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote
May 2000 **Proceedings of the 2000 annual national conference on Digital**

government research dg.o '00
Publisher: Digital Government Research Center
Full text available: pdf(539.99 KB) Additional Information: full citation, abstract

As use of the Internet in commerce, education and personal communication has become common, the question of Internet voting in local and national elections naturally arises. In addition to adding convenience and precision, some believe that Internet voting may reverse the historical and downward trend of voter turnout in the United States. For these reasons President Clinton issued a memorandum in December 1999 requesting that the National Science Foundation examine the feasibility of online (In ...

13 Internet Privacy Enhanced Mail

Stephen T. Kent
August 1993 **Communications of the ACM**, Volume 36 Issue 8
Publisher: ACM Press
Full text available: pdf(4.82 MB) Additional Information: full citation, references, citings, index terms, review

Keywords: Internet Privacy Enhanced Mail

14 Just fast keying: Key agreement in a hostile internet

William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2
Publisher: ACM Press
Full text available: pdf(324.39 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of tradeoffs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

15 Using certified policies to regulate E-commerce transactions

Victoria Ungureanu
February 2005 **ACM Transactions on Internet Technology (TOIT)**, Volume 5 Issue 1
Publisher: ACM Press
Full text available: pdf(404.92 KB) Additional Information: full citation, abstract, references, citings, index terms, review

E-commerce regulations are usually embedded in mutually agreed upon contracts. Generally, these contracts enumerate agents authorized to participate in transactions, and spell out such things like rights and obligations of each partner, and terms and conditions of the trade. An enterprise may be concurrently bound by a set of different contracts that regulate the trading relations with its various clients and suppliers. This set is dynamic because new contracts are constantly being established, ...

Keywords: Contract terms, Enforcement, Scalability

16 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: pdf(118.52 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

17 Internet security standards: past, present, and future

Stephen Kent

June 1994 **StandardView**, Volume 2 Issue 2

Publisher: ACM Press

Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings, index terms

18 Genealogical approaches to ethical implications of informational assimilative integrated discovery systems (AIDS) in business

Kamal Dean Pharhizgar, Stephen E. Lunce

November 1994 **Proceedings of the conference on Ethics in the computer age**

Publisher: ACM Press

Full text available: pdf(694.25 KB) Additional Information: full citation, abstract, references, index terms

Development of knowledge-based technological acquisition techniques and customers' information profiles are known as assimilative integrated discovery systems (AIDS) in modern organizations. These systems have access through processing to both deep and broad domains of information in modern societies. Through these systems organizations and individuals can predict future trend probabilities and events concerning their customers. AIDSs are new techniques which produce new information which i ...

19 Viewpoint: One more revolution to make: free scientific publishing

Krzysztof R. Apt

May 2001 **Communications of the ACM**, Volume 44 Issue 5

Publisher: ACM Press

Full text available: pdf(72.37 KB) html(21.95 KB) Additional Information: full citation, references, index terms

20 COCA: A secure distributed online certification authority

Lidong Zhou, Fred B. Schneider, Robbert Van Renesse

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player